

DATABEHANDLERAFTALE

Denne databehandleraftale (herefter "Aftalen") er indgået på tidspunktet for parternes behørigt underskrift herpå

mellem

KUNDEN

og

COMAsystem ApS Ringager 8

2605 Brøndby

CVR-nr. 33 86 52 79

(herefter "Leverandøren")

Kunden og Leverandøren er samlet benævnt "Parterne" og separat tillige en "Part".

AFTALENS OMFANG

Leverandøren er databehandler for Kunden, idet Leverandøren varetager de i Appendiks 1 beskrevne databehandlingsopgaver på vegne af Kunden og udelukkende efter klar instruks fra Kunden.

De personoplysninger, der behandles af Leverandøren, omfatter de formål med behandlingen, de kategorier af personoplysninger og de kategorier af registrerede personer, som er anført i Appendiks 1.

Ved "personoplysning" forstås enhver form for information om en identificeret eller identificerbar fysisk person, jf. artikel 4(1) i Forordning (EU) 2016/679 af 27. april 2016 ("persondataforordningen"). Hvis der som led i opfyldelsen af Aftalen behandles andre fortrolige oplysninger end personoplysninger, for eksempel oplysninger som i medfør af lov om finansiel virksomhed anses for fortrolige, så omfatter enhver henvisning til "personoplysninger" også de øvrige fortrolige oplysninger.

1 BEHANDLING AF PERSONOPLYSNINGER

- 1.1 Instruks: Leverandøren er instrueret i alene at behandle personoplysningerne med det formål at varetage de i Appendiks 1 fastsatte databehandlingsopgaver. Leverandøren må ikke behandle eller anvende personoplysningerne til andre formål end angivet i instruksen, herunder overføre personoplysningerne til et tredjeland eller en international organisation, medmindre Leverandøren er forpligtet hertil efter EU-retten eller lovgivningen i en medlemsstat, som Leverandøren er underlagt. I givet fald skal Leverandøren skriftligt underrette Kunden om denne juridiske forpligtelse, forinden behandlingen påbegyndes, medmindre pågældende lovgivning på baggrund af vigtige samfundsinteresser forbyder en sådan underretning.
- 1.2 Hvis Kunden i instruksen i Appendiks 1 eller konkret har givet tilladelse til en overførsel af personoplysninger til et tredjeland eller til internationale organisationer, påhviler det Leverandøren at sikre, at der foreligger et lovligt overførselsgrundlag, f.eks. EU Kommissionens standardkontrakter til overførsel af personoplysninger til tredjelande.
- 1.3 Hvis Leverandøren skønner, at en instruktion fra Kunden er i strid med persondataforordningen eller databeskyttelseslovgivningen i anden EU-ret eller i lovgivningen i en medlemsstat, skal Leverandøren omgående skriftligt orientere Kunden herom.
- 1.4 Kunden er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med gældende persondataret, herunder databeskyttelsesforordningen (se forordningens artikel 24), relevante databeskyttelsesbestemmelser i anden EU-ret eller EØS-medlemsstaternes nationale ret og denne Aftale.
- 1.5 Kunden har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.

Kunden er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.

2 KRAV TIL LEVERANDØREN

- 2.1 Leverandøren skal sikre, at de personer, der er autoriseret til at behandle personoplysningerne, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.
- 2.2 Leverandøren skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at de behandlede personoplysninger
- I hændeligt eller ulovligt tilintetgøres, fortabes eller ændres,
 - II videregives eller gøres tilgængelige uden autorisation, eller
 - III i øvrigt behandles i strid med lovgivningen, herunder persondataforordningen.
- 2.3 Leverandøren skal desuden overholde de særlige krav til sikkerhedsforanstaltninger, der gælder for Kunden, jf. Appendiks 1, samt overholde de krav til sikkerhedsforanstaltninger, som direkte forpligter Leverandøren, herunder kravene til sikkerhedsforanstaltninger i det land hvor databehandlingen finder sted.
- 2.4 Fastsættelsen af de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger skal ske under hensyntagen til
- I det aktuelle tekniske niveau,
 - II omkostningerne ved implementeringen,
 - III samt behandlingens karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder.
- 2.5 Leverandøren skal på Kundens anmodning give Kunden alle nødvendige oplysninger til, at denne kan påse, at Leverandørens forpligtelser under Aftalen overholdes, herunder at de nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger er truffet.
- 2.6 Leverandøren skal hvert år i december for egen regning indhente en erklæring fra en uafhængig ekspert angående Leverandørens overholdelse af kravene til sikkerhedsforanstaltninger fastsat i Aftalen. Erklæringen skal udarbejdes på grundlag af en anerkendt standard for sådanne erklæringer. Erklæringen skal sendes til Kunden senest den 31. december det pågældende år.
- 2.7 Derudover har Kunden ret til for egen regning at udpege en uafhængig ekspert, som skal have adgang til Leverandørens fysiske faciliteter for behandling af personoplysninger samt modtage de nødvendige informationer til udførelsen af undersøgelsen af, hvorvidt Leverandøren har truffet de nævnte tekniske og organisatoriske sikkerhedsforanstaltninger. Eksperten skal på Leverandørens anmodning underskrive en sædvanlig fortrolighedserklæring for at få adgang til Leverandørens faciliteter og de ovenfor nævnte oplysninger og behandle enhver information indhentet hos eller modtaget direkte fra Leverandøren strengt fortroligt og må alene dele informationen med Kunden og må ikke anvende informationen til noget andet formål.

2.8 Leverandøren skal til myndigheder og Kundens eksterne rådgivere, herunder revisorer, for Kundens regning give alle ønskede oplysninger i relation til udførelsen af databehandlingsopgaven, i det omfang oplysningerne er nødvendige for deres opgavevaretagelse i medfør af EU-retten eller lovgivningen i en medlemsstat.

2.9 Leverandøren skal give myndigheder, der efter EU-retten eller lovgivningen i en medlemsstat har adgang til Kundens og Kundens leverandørers faciliteter, eller repræsentanter, der optræder på myndighedernes vegne, adgang til Leverandørens fysiske faciliteter mod forevisning af behørig legitimation.

2.10 Leverandøren skal uden unødigt forsinkelse og aldrig senere end 24 timer efter at være blevet opmærksom herpå, skriftligt orientere Kunden om

- I enhver anmodning fra en myndighed om videregivelse af personoplysninger omfattet af Aftalen, medmindre orientering af Kunden er forbudt i henhold til EU-retten eller lovgivningen i en medlemsstat,
- II enhver mistanke om, eller konstatering af, (a) brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet af Leverandøren under Aftalen, eller (b) enhver anden manglende overholdelse af Leverandørens forpligtelser efter punkt 2.1 og 2.2, eller
- III enhver anmodning om indsigt i personoplysningerne modtaget direkte fra den registrerede eller fra tredjemand.

2.11 Leverandøren skal straks assistere Kunden med håndteringen af enhver anmodning fra en registreret under kapitel III i persondataforordningen, herunder anmodning om indsigt, berigtigelse, blokering eller sletning af personoplysninger. Såfremt sådan bistand overstiger almindelig support, sker denne bistand efter forudgående skriftlig godkendelse, for Kundens regning. Leverandøren skal ligeledes implementere passende tekniske og organisatoriske foranstaltninger til at bistå Kunden med opfyldelse af Kundens forpligtelse til at besvare sådanne anmodninger.

2.12 Leverandøren skal for Kundens regning assistere Kunden med at overholde de øvrige forpligtelser, der måtte påhvile Kunden efter EU-retten eller lovgivningen i en medlemsstat, hvor Leverandørens assistance er forudsat, samt hvor Leverandørens assistance er nødvendig for, at Kunden kan overholde sine forpligtelser. Dette omfatter blandt andet, men er ikke begrænset til, på anmodning at give Kunden alle nødvendige oplysninger om en hændelse omfattet af punkt 2.9 (ii), samt alle nødvendige oplysninger til brug for en konsekvensanalyse i medfør af artikel 35-36 i persondataforordningen (forordning (EU) 2016/679 af 27. april 2016).

- 2.13 I Appendiks 1 har Leverandøren oplyst den fysiske placering af servere, servicecentre mv., som indgår i udførelsen af databehandlingen. Leverandøren forpligter sig til at give skriftligt varsel til Kunden mindst 2 måneder forud for ændringer af den fysiske placering. Dette kræver ikke en formel ændring af Appendiks 1, idet forudgående skriftligt varsel via post eller e-mail er tilstrækkeligt. Såfremt Kunden måtte have sag- lige og rimelige indvendinger mod en sådan fysisk ændring, skal Kunden være berettiget til at nægte ændringen. Hvis lokationen medfører overførsel af personoplysninger til områder uden for EU/EØS, skal Leverandøren forud for påbegyndelse af enhver sådan overførsel indhente Kundens skriftlige godkendelse heraf.

3 ANDRE DATABEHANDLERE

- III.1 Leverandøren skal være berettiget til at anvende underdatabehandlere til udførelse af visse eller alle af Leverandørens opgaver i henhold til denne Aftale. Leverandøren skal oplyse Kunden om brugen af en bestemt underdatabehandler. Kunden skal være berettiget til at gøre indsigelse mod brugen af den specifikke, nye underdatabehandler. Ved ophør af brugen af den anden databehandler, skal Leverandøren give Kunden skriftlig meddelelse herom.
- III.2 Leverandøren skal forinden brug af en anden databehandler indgå en skriftlig aftale med den anden data- behandler, hvori den anden databehandler som minimum pålægges de samme forpligtelser, som Leve- randøren har påtaget sig ved Aftalen, herunder pligten til at gennemføre passende tekniske og organisatoriske foranstaltninger til sikring af, at behandlingen opfylder kravene i persondataforordningen.
- III.3 Kunden har ret til at få udleveret en kopi af Leverandørens aftale med den anden databehandler, for så vidt angår bestemmelser i nævnte aftale, som vedrører databeskyttelsesforpligtelser. Leverandøren hæfter over for Kunden for underleverandørens opfyldelse af sine databeskyttelsesforpligtelser. Det forhold, at Kunden har meddelt samtykke til Leverandørens aftaleindgåelse med en anden databehandler, er uden præjudice for Leverandørens pligt til at efterleve Aftalen.

4 FORTROLIGHED

- 4.1 Leverandøren skal holde personoplysningerne fortrolige.
- 4.2 Leverandøren må ikke formidle personoplysningerne til tredjemand, medmindre dette er nødvendigt til varetagelse af Leverandørens forpligtelser over for Kunden i henhold til Aftalen og forudsat, at den, til hvem personoplysningerne overlades, er bekendt med oplysningernes fortrolige karakter og har indvilget i at holde personoplysningerne fortrolige i overensstemmelse med Aftalen.
- 4.3 Leverandøren skal sikre, at Leverandørens medarbejdere overholder fortrolighedsforpligtelserne i Aftalen.

- 4.4 Leverandøren skal begrænse adgangen til personoplysninger til de medarbejdere, for hvem det er nødvendigt at have adgang dertil for at kunne opfylde Leverandørens forpligtelser over for Kunden.
- 4.5 Leverandørens forpligtelser efter nærværende punkt 4 består uden tidsbegrænsning, og uanset om Par- ternes samarbejde i øvrigt måtte være ophørt.

5 ÆNDRINGER OG OVERDRAGELSER

- 5.1 Parterne kan til enhver tid aftale at ændre Aftalen. Ændringer skal være skriftlige for at være gyldige.
- 5.2 Leverandøren må ikke overdrage sine rettigheder og forpligtelser i henhold til Aftalen uden Kundens for- udgående skriftlige samtykke.

6 VARIGHED OG OPHØR AF AFTALEN

- 6.1 Aftalen træder i kraft ved begge Parters underskrift og er gældende, indtil den opsiges eller op- hæves af en af Parterne i overensstemmelse med bestemmelserne derom i denne Aftale.
- 6.2 Hver Part kan opsiges Aftalen med 3 måneders skriftligt varsel.
- 6.3 Uanset Aftalens formelle aftaleperiode skal Aftalen vedblive at gælde, så længe Leverandøren behandler de personoplysninger, som Kunden er dataansvarlig for.
- 6.4 I tilfælde af ophør af Aftalen, uanset det juridiske grundlag herfor, skal Leverandøren yde de fornødne overgangstjenesteydelser til Kunden. Såfremt sådan bistand overstiger almindelig support, sker denne bistand efter forudgående skriftlig godkendelse, for Kundens regning. Le- verandøren er forpligtet til loyalt og hurtigst muligt at medvirke til, at databehandlingen overgår til en anden leverandør eller tilbageføres til Kunden.
- 6.5 Leverandøren skal straks efter anmodning fra Kunden overføre eller slette personoplysninger, som Leve- randøren behandler for Kunden, medmindre EU-retten eller lovgivningen i en med- lemsstat foreskriver opbevaring af de pågældende personoplysninger. Modtager Leverandøren ingen sådan anmodning fra Kunden, skal Leverandøren slette alle personoplysninger, som Le- verandøren behandler for Kunden, se- nest 6 måneder efter Aftalens ophør. Sletteperioden om- fatter udløb af retention for inaktive filer i backup.

7 FORRANG

- 7.1 I tilfælde af uoverensstemmelse mellem bestemmelserne i denne Aftale og bestemmelserne i andre skriftlige eller mundtlige aftaler indgået mellem Parterne, skal bestemmelserne i denne Aftale have for- rang. Bestemmelserne i punkt 2 finder dog ikke anvendelse i det omfang, der er fastsat strengere forpligtelser for Leverandøren ved anden aftale mellem Partnerne. Herud- over finder Aftalen ikke anvendelse i det omfang, der er fastsat strengere forpligtelser for Leve- randøren eller dennes underleverandører ved brug af Kommissionens standardkontrakter til overførsel af personoplysninger til tredjelände.



APPENDIKS 1

DETTE APPENDIKS UDGØR KUNDENS INSTRUKS TIL LEVERANDØREN I FORBINDELSE MED LEVERANDØRENS DATABEHANDLING FOR KUNDEN, OG ER EN INTEGRERET DEL AF AFTALEN.

BEHANDLINGEN AF PERSONOPLYSNINGER

FORMÅL OG KARAKTEREN AF DATABEHANDLINGEN

Leverandøren varetager opbevaring og behandling af kundens kontraktdata, der indeholder personhenførbare oplysninger.

Leverandøren opbevarer kundens kontraktfiler og dokumenter, inkl. de af kundens selv indtastede oplysninger. Leverandøren foretager email-alarmering til kunden på baggrund af de af kunden angivne forhold.

Leverandøren sletter data med automatiserede processer på baggrund af de af kunden angivne forhold.

Leverandøren har under ingen omstændighed mulighed for at dele kundens oplysninger med tredjepart, med undtagelse af udefrakommende retskrav.

Leverandøren må ikke anvende og eller behandle kundens data ifm. interne formål hos Leverandøren.

KATEGORIER AF REGISTREREDE PERSONER

Medarbejder	[X]
Ansøger	[X]
Leverandører	[X]
Kunder	[X]

KATEGORIER AF PERSONOPLYSNINGER

Følgende kategorier er kun gældende når kunden anvender personalemodulet i leverandørens system.

Følsomme personoplysninger [X]

fagforeningsmæssige forhold

helbredsoplysninger

Almindelige personoplysninger [X]

Økonomiske forhold

Bil

Skat

CPR (nationalt fortroligt)

Følgende kategorier er gældende når kunden anvender en eller flere af følgende moduler i leverandørens system:

Køb

Salg

Service

Almindelige personoplysninger

[X]

Navn

Adresseoplysninger

Telefon

Email

Stilling

CVR

Ovenstående er det tilsigtede udgangspunkt. Listen er dog ikke nødvendigvis udtømmende og kan omfatte yderligere oplysninger, hvis kunden selv lægger andre typer oplysninger ind i systemet.

Systemet kan anvendes til alle almindelige og følsomme oplysninger, men det er kunden som vælger hvilke oplysninger der lægges ind i leverandørens system.

LOKATION(ER), INKLUSIVE ANGIVELSE AF LAND FOR BEHANDLINGEN

Leverandøren driver egen hosting af både hardware og software i en datacenterlokation hos Global Connect. Data er placeret på Hørskættø, Høje Taastrup, Sjælland, Danmark.

Global Connect stiller alene de fysiske faciliteter (bygning) til rådighed for Leverandøren, og Global Connect har ikke adgang til Kundens data og er ikke (under)databehandler.

UNDERDATABEHANDLERE

Generel DRIFT & UDVIKLING:

Underdatabehandler:

Nordicode ApS – Udvikling

CVR.: 39030845

Nørre Voldgade 18, 1 1358 København K



Underdatabehandler:

Front-Safe A/S – Backup

CVR.: 29631123

Spotorno Allé 12 2630 Taastrup

Søndervangs Alle 20 8260 Viby

Underdatabehandler :

Visma Consulting A/S – Digital underskrift

CVR.: 29973334

Nørgaardsvej 32 2800 Lyngby

Denne databehandler varetager kun behandling af persondata for kunder, som anvender digital signaturfunktionen igennem Leverandøren.

Databehandler under Privacy Shield ordning:

INGEN

SIKKERHED OG RAPPORTERING AF DATABRUD

Som led i Leverandørens etablering af passende tekniske og organisatoriske foranstaltninger, skal Leverandøren vurdere det nødvendige sikkerhedsniveau ud fra karakteren og omfanget af behandlingen og indrette behandlingssikkerheden ud fra det til enhver tid fastlagte sikkerhedsniveau. Leverandøren skal som minimum følge den angivne instruks i appendix 2 vedlagt som "Instruks om etablering af tekniske og organisatoriske foranstaltninger", som ændret fra tid til anden.

Appendix 2 til Appendix 1

Instruks om etablering af

Tekniske og organisatoriske foranstaltninger

Specifikke tekniske og organisatoriske sikkerhedskrav:

Der stilles følgende specifikke minimumskrav til Databehandlerens sikkerhed:

Informationssikkerhedspolitik

Databehandleren skal sikre, at der foreligger en ledelsesgodkendt informationssikkerhedspolitik.

Organisering af informationssikkerhed

Databehandleren skal sikre, at der er fokus på informationssikkerheden i egen organisation med defineret rolle- og ansvarsfordeling.

Desuden skal Databehandlerens dataadgange til den Dataansvarliges data sikres gennem kontrakter, fortrolighedserklæring samt sikring af funktionsadskillelse for at minimere fejl og misbrug af data.

Medarbejdersikkerhed

Databehandleren skal have etableret en proces for at medarbejdere og konsulenter kender deres ansvar i forhold til informationssikkerhed.

Databehandleren skal udføre awareness vedrørende medarbejderes forpligtelser ved ansættelse og denne træning skal vedligeholdes hele ansættelsesforholdets varighed.

Styring af aktiver

Databehandleren skal sikre ejerskab af kritiske aktiver og opdateret dokumentation.

Adgangsstyring

Databehandleren skal have en dokumenteret adgangsstyringsproces og sikre at adgange alene tildeles på baggrund af et arbejdsbetinget behov.

Databehandleren skal have etableret procedurer for oprettelse, nedlæggelse og løbende gennemgang af tildelte rettigheder ud fra princippet om et arbejdsbetinget behov samt stillingtagen til funktionsadskillelse.

Databehandleren skal have procedurer for sikker log-on for at minimere mulighederne for uautoriseret adgang til systemer og applikationer.



Kryptografi

Databehandleren skal sikre kryptering med tidssvarende krypteringsniveau ved kommunikation over åbne net og mellem systemer samt sikre at administration af nøgler sker efter en dokumenteret proces.

Fysisk sikring og miljøsikring

Databehandleren skal tilrettelægge og etablere fysisk beskyttelse mod naturkatastrofer, ondsindede angreb eller ulykker af Databehandlerens fysiske lokationer.

Databehandleren skal desuden sikre beskyttelse mod uautoriseret adgang til Databehandlerens fysiske lokationer via proces for adgangskontrol for alle med adgang.

Driftssikkerhed

Databehandleren skal sikre, at driftsprocedurer dokumenteres og vedligeholdes. Som minimum skal følgende procedurer omfattes:

- malware beskyttelse
- backup
- logging og overvågning
- styring af driftssoftware
- sårbarhedsstyring

Kommunikationssikkerhed

Databehandleren skal sikre, at netværk styres og kontrolleres for at beskytte informationer. Databehandleren skal sikre, at den Dataansvarliges data, der kommunikeres internt og eksternt, behandles korrekt lovgivningsmæssigt, etisk og forretningsmæssigt i informationernes levetid. Derudover skal adgange til netværket beskyttes.

Anskaffelse, udvikling, vedligeholdelse og bortskaffelse af systemer

Databehandleren skal sikre, at sikkerhedskrav ved anskaffelse, udvikling, vedligeholdelse og bortskaffelse integreres i løsningerne, samt at Databeskyttelsesforordningens krav om databeskyttelse gennem design og standardindstillinger iagttages.

Ændringer i systemer

Databehandlerens skal sikre, at ændringer i it-systemer følger en dokumenteret ændringsproces med relevante godkendelser og test.

Databehandleren skal sikre at udviklings-, test- og driftssystemer holdes adskilt samt at kapacitet og ydeevne overvåges og styres.

Leverandørforhold

Databehandleren skal stille mindst samme sikkerhedskrav til Underdatabehandlere og øvrige underleverandører, som gælder for Databehandleren og sikre efterlevelse af disse.

Styring af informationssikkerhedsbrud

Databehandleren skal registrere og risikovurdere informationssikkerhedshændelser og rapportere disse til den Dataansvarlige uden ugrundet ophold. Databehandleren skal udarbejde procedurer for bevisindsamling ved informationssikkerhedshændelser.

Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Databehandleren skal have udarbejdet beredskabsplaner, der definerer hvordan systemer eller services rettidigt reetableres. Disse beredskabsplaner skal testes årligt eller ved større ændringer.

Overensstemmelse (Compliance)

Databehandleren skal regelmæssigt undersøge, om systemer og services lever op til Databehandlerens sikkerhedsmæssige krav samt sikkerhedskravenes effektivitet og evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af systemer og services.
